Before the
FEDERAL COMMUNICATIONS COMMISSION
Washington, D.C. 20554

In the Matter of	)	
	)	
Cyber Security Certification Program	)	PS Docket No. 10-93
	)	

To: The Commission

REPLY COMMENTS OF HARRIS CORPORATION

This filing is submitted on behalf of Harris Corporation ("Harris") before the Federal Communications Commission ("Commission") in response to the Commission's *Notice of Inquiry* seeking comment on whether the Commission should establish a voluntary program under which participating communications service providers would be certified by the Commission or a third party entity for their adherence to a set of cyber security objectives.[1] In general, the Commission seeks comment on the components of such a program, if any, and whether such a program would create business incentives for providers of communications services to sustain a high level of cyber security culture and practice. Through Harris' experience in the construction, management, and protection of broadband communications networks, Harris by its Cyber Integrated Solutions Business Unit, is in a highly qualified position to provide the Commission with input regarding the state of broadband network security and the viability of a voluntary certification program. Harris takes this opportunity to discuss: (1) the challenges posed by the government running and coordinating a cyber security certification

[1] In the Matter of Cyber Security Certification Program, *Notice of Inquiry*, PS Docket No. 10-93, 25 FCC Rcd. 4345 (rel. Apr. 21, 2010) ("Certification NOI").

program and (2) how Commission action may not be appropriate at this time as it could mitigate current industry cyber security efforts.

Before instituting new cyber security initiatives Harris encourages the Commission to evaluate existing industry efforts[2] and how industry driven programs may already be accomplishing the same goals laid out in the Commission's *Notice of Inquiry*.[3] Harris believes that a government run certification program that crosscuts industry may not be the most appropriate means to address cyber security issues given the diverse landscape of broadband services, the always changing environment of cyber security threats, and the unique cyber security needs of varying industry sectors serviced by broadband providers. Industry should have the ability to provide a full range of unique cyber security offerings to address disparate industry sectors' cyber security needs and requirement sets.[4] Harris, through the work of its Cyber Integrated Solutions Business Unit, is working to address the unique cyber security needs of numerous industry sectors.

I. Harris Has An Extensive Background in Network Construction, Management, and Security and Is in the Process of Establishing the Nation's First Cyber Integration Center.

Harris is an international communications and information technology company, headquartered in Melbourne, Florida, that serves government and commercial markets in more

[2] "Substantial incentives exist for communications providers to continually improve their cyber security practices, as many large business and government customers are educated on cyber security policies and providers will and do lose those customers if cyber attacks against their networks are successful." Comments of AT&T Inc., In the Matter of Cyber Security Certification Program, PS Docket No. 10-93, pg. 13 (filed July 12, 2010) ("Comments of AT&T").

[3] "Our goals in this proceeding are: (1) to increase the security of the nation's broadband infrastructure; (2) to promote a culture of more vigilant cyber security among participants in the market for communications services; and (3) to offer end user more complete information bout their communication service provider's cyber security practices." Certification NOI, *supra* note 1, at 4346, ¶ 1.

[4] "There is no evidence that communications and other industries are not able or willing either to create their own cyber security standards and certifications or to adopt existing ones." Comments of the Mercatus Center at George Mason University, In the Matter of Cyber Security Certification Program, PS Docket No. 10-93, pg. 2 (filed July 12, 2010). ("Comments of George Mason").

than 150 countries. For decades Harris has used state-of-the-art technology assessment techniques and architecture engineering design methods to define, deliver, operate, and secure communications networks. Harris technology, countermeasures, and monitoring capabilities have effectively safeguarded vital information systems that support the critical missions of military, intelligence, and local and federal law enforcement customers. Harris operates some of our nation's largest and most secure, mission-critical networks.

For example, since 2002 Harris has performed as the prime contractor on the 15-year Federal Aviation Administration ("FAA") Federal Telecommunications Infrastructure ("FTI") program to integrate and modernize the U.S. air traffic control system and infrastructure. FTI is a modern, secure, and efficient network that provides voice, data, and radar communications to more than 4,000 FAA and Department of Defense sites across the country (including Alaska, Hawaii, and Puerto Rico). The FTI program has helped to reduce overall FAA operating costs while enhancing network efficiency, reliability, security, and service. In February 2008 Harris successfully completed the transition of FAA legacy networks to the new FTI network.

Harris is utilizing its understanding of communications networks and applications to develop innovative solutions to ensure security and reliability across broadband networks in the government and a wide range of private industries. One such innovative solution is Harris' plan to build the nation's first Cyber Integration Center, which will provide government and commercial customers with a unique secure managed hosting service in a trusted environment. The Harris Cyber Integration Center will provide customers with an innovative on-demand integrated offering of infrastructure, managed security, tailored hosting and services—all provided as a secure, trusted total solution. The Center will feature a LEED Certified facility and trusted technology infrastructure, which delivers a highly reliable, automated, and highly elastic

multi-tenant cloud computing environment with secure supply chain integrity, and advanced persistent threat deterrence. By offering industry-tailored secure hosting solutions and services on a tiered structure, customers will benefit from both flexibility of an extremely secure, on-demand service coupled with superior client services and value. The Cyber Integration Center will be located in the Mid-Atlantic region. Harris is aiming to have the Center fully operational by the end of the 2010 calendar year.

II. Implementing a Voluntary Certification Program Will Be Resource Intensive and Difficult for Government to Maintain.

The management overhead necessary for the Commission to track potentially thousands of certifications would likely demand an extremely large amount of human and financial capital, including training, database creation and maintenance, data storage and archiving, project planning, certification application tracking, and program compliance. A government run certification regime would also likely have the unintentional effect of driving up the market demand for an already stretched pool of certified IT practitioners. Even a voluntary certification program would likely cost the United States government millions of dollars to meet the resource demands of the program, regardless of whether the program is in sourced or outsourced to a third party vendor.

Today, technologies are extremely dynamic as are their related security vulnerabilities.[5] Services are more diverse than ever and "intelligent devices supports a wider range of flexible, customized, and multimedia services."[6] Networks have become more interconnected making it

[5] *See* Comments of Telecommunications Industry Association, In the Matter of Cyber Security Certification Program, PS Docket No. 10-93, pgs. 4-5 (filed July 12, 2010) (discussing the IT Sector Coordinating Council findings on incentives for encouraging cyber security best practices and the conclusion on how requirements differ based upon an entities unique needs and risk profile).

[6] Comments of Telcordia, In the Matter of Cyber Security Certification Program, PS Docket No. 10-93, pg. 3 (filed July 12, 2010).

difficult to apply a single set of standards to address cyber security concerns.[7] Varying levels of knowledge are required by cyber security professionals regarding the compliance standards necessary to evaluate the technical proficiency of a particular network provider's chosen method for protecting their network and securing data across their network. Keeping up with changes in security procedures and threats to keep a certification program relevant will require a significant commitment of resources. Commenters accurately recognized that any program criteria would quickly become out-of-date and require constant review.[8] Due to the commitment of resources needed to maintain an industry-wide certification program, such efforts may be more appropriately undertaken by industry or independent third party vendors, as opposed to the government. [9]

As an example of ongoing industry led efforts, Harris is currently collaborating with key industry leading vendors as well as cyber security policy and standard making bodies to establish strong formalized partnerships that leverage existing vendor expertise and encourage implementation of cyber security best practices. Harris' Cyber Integrated Solutions' business offerings will be supported by a foundational roadmap that encompasses cyber security certification and compliance goals as set forth by the National Institute of Standards and Technology ("NIST"), the International Organization for Standardization ("ISO"), Department of Defense ("DoD"), Department of Health & Human Services ("HHS"), the Payment Card

[7] "The entire concept of interconnection has evolved to include not just service provider-to-service provider, but also service provider-to-clouds and service provider-to-large enterprises. All of these types of interconnection and access arrangements, as well as ever smarter devices and advanced services, serve to increase available avenues for attack through both traditional and emerging vulnerabilities." Id.

[8] "Any certification program assessment of cyber security would quickly become out-of-date." Comments of the Alliance for Telecommunications Industry Solutions, In the Matter of Cyber Security Certification Program, PS Docket No. 10-93, pg. 6 (filed July 12, 2010).

[9] "Given the evolving nature of broadband networks and technologies, ATIS does not believe that any certification program could provide an accurate and up-to date assessment of security." Id., at 5.

Industry Security Standards Council ("PCISS"), and the Auditing Standards Board of the American Institute of Certified Public Accountants, just to name a few. Harris' Cyber Integrated Solution's business offerings will also be compliant with numerous government standards, such as NIST Special Publication 800-53, ISO 20000, ISO 27001, the DoD Information Assurance Certification and Accreditation Process, the HHS Health Insurance Portability & Accountability Act (HIPAA), the HHS Health Information Technology for Economic and Clinical Health (HITECH) Act, and the Payment Card Industry Data Security Standard.

Establishing a foundational roadmap prior to providing services will allow Harris to deliver to our customers a secure infrastructure that is planned, designed, implemented, and operated by an elite cadre of certified cyber security professionals who are trained and vetted through existing industry and government based security standards that meet the unique needs of a particular customer. The foundational roadmap will also enable Harris to train and certify cyber security professionals who understand the unique needs of a particular customer's industry. Such a knowledge base will allow Harris cyber security professionals to ensure the confidentiality, integrity, and availability of our customer's infrastructure and data by staying in front of new technology developments, cyber security threats, and cyber security vulnerabilities.

III. Commission Action May Mitigate Efforts Already Being Undertaken by Industry to Address the Unique Needs of Specific Industry Sectors.

Existing industry efforts, both independent and public-private partnerships, provide diverse solution sets to addressing current and emerging cyber security challenges.[10] To implement a successful certification program a flexible, easily modified evaluation process based

[10] "ATIS also believes that, given the significant work underway in the industry related to cyber security, such a program is not necessary to enhance existing security practices." Id., at 3; S*ee also* Comments of Verizon and Verizon Wireless, In the Matter of Cyber Security Certification Program, PS Docket No. 10-93, pgs. 6-8 (filed July 12, 2010) (providing four examples of how Verizon and Verizon Wireless has independently addressed cyber security challenges); S*ee also* Comments of AT&T, *supra* note 2, at 8-13 (highlighting both private-public partnerships and independent solutions AT&T provides directly to customers).

on unique criteria is needed, as opposed to a rigid process based around generic, non specific, network standards, requirements, and threats. A process driven by specific industries will provide the flexibility needed to take into account the diverse nature of addressing modern cyber security issues and help promote innovative solutions to addressing new cyber security threats. From a practical level it would be difficult for a government run certification scheme to provide the flexibility necessary to address current and emerging threats.[11] Industry and third party vendors can more easily account for advances in technology and address unique industry specific network cyber security requirements and priorities.

The Commission should take under advisement that in such a dynamic technological world there is no "one size fits all" approach to cyber security. In fact, a government run program may actually hinder efforts to meet the demands of a constantly evolving environment by encouraging service providers to only focus on a narrow set of requirements identified by the government or the lowest common denominator.[12] The establishment of a list of government cyber security requirements, even voluntary, could result in a slippery slope that unintentionally discourages new cyber security prevention methods to address emerging threats and limits the development of innovative cyber security solutions, applications, and approaches.

---

[11] "If certification requirements are high level enough to be acceptable by all parties, they risk to drive toward adoption of minimum requirements/best practices rather than the most robust secure solutions/practices available." Id.

[12] "It is more effective to allow private enterprise to develop protections for rapidly emerging and evolving threats, rather than encouraging them to devote resources to comply with certification standards that may become outdated. Allowing industry the flexibility to develop fluid and responsive security measures will promote innovative discovery that may be hindered by a Commission certification program. Another concern of such a program is that it may discourage innovation outside the scope of certification. Much as teachers evaluated predominantly by test scores of their students will often "teach to the test," a Commission certification program could encourage communications service providers to concentrate solely on complying with acquiring the certificate, this hindering other security innovations. The Commission should be aware of the potential to discourage security innovation outside the bounds of its program by implying, indirectly, that its standards are sufficient." Comments of George Mason, *supra* note 4, pgs. 3-4.

As previously mentioned, Harris is already taking steps to address cyber security concerns through a full range of unique cyber security offerings to meet various industry sectors' needs and requirements. Whether cyber security criteria are set in policy, vendor partnership agreements, or stipulated by law, Harris can provide ISO certified internal and external auditing processes to provide for program transparency, confirm cyber security claims. Certification documentation will be maintained and available to provide customers with proof of compliance. In addition, Harris will maintain a robust educational incentive program that rewards cyber security professionals for obtaining and retaining relevant cyber security certifications and knowledge. This robust list of cyber security courses and certifications will be reviewed for accuracy and relevance on a continuous basis.

The Commission may be better served at this time by continuing to emphasize compliance with standard setting bodies, conducting periodic reviews of the state of the cyber security industry, interfacing with other government agencies to create uniform standards, and taking steps to promote a culture of diligent and informed cyber security practices amongst consumers. Commenters have identified numerous manners in which the federal government (including the Commission) can work to promote such practices.[13] For example, the federal government could: (1) leverage its purchasing power to create incentives for companies that do business with the government to adopt high level cyber security practices; (2) extend grants to

[13] *See* Comments of Sprint Nextel Corporation, In the Matter of Cyber Security Certification Program, PS Docket No. 10-93, pgs. 10-12 (filed July 12, 2010) (recommending steps the Commission can take to advance its cyber security goals instead of a certification program, including continued support of the Communications Security, Reliability and Interoperability Council and consumer education/outreach); *See also* Comments of AT&T, *supra* note 10, at 25-29 (proposing a comprehensive education and outreach campaign to inform consumers about security best practices and how to protect themselves and their sensitive information); *See also* Comments of the United States Telecom Association, In the Matter of Cyber Security Certification Program, PS Docket No. 10-93, pgs. 17-19 (filed July 12, 2010) (advocating for additional federal funding to further encourage private sector innovation and investment in cyber security efforts).

companies developing and implementing cyber security technologies and practices; and (3) harmonize cyber security policy and efforts to eliminate inefficiencies or redundancies.

IV. Conclusion

Harris respectfully requests that the Commission take into account the recommendations set forth in these Reply Comments when considering whether to establish a cyber security certification program. Harris stands ready to work with both the public and private sector to provide innovative solutions, such as Harris' Cyber Integration Center, to effectively secure cyberspace and the nation's broadband infrastructure.

Respectfully submitted,

HARRIS CORPORATION
600 Maryland Avenue, S.W.
Suite 850E
Washington, D.C. 20024
(202) 729-3700

/s/

Carl M. Bradley
Sales Engineer, Cyber Integrated Solutions

Evan S. Morris, Esq.
Legal Analyst, Government Relations

September 8, 2010